PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified MEHARI

The objective of the “PECB Certified MEHARI Risk Manager” examination is to ensure that the candidate has the knowledge and the skills to support an organization to identify, analyze, prioritize and manage information security risks. Furthermore, the objective of this examination is to ensure that the candidate also has the knowledge and the skills to support an organization in implementing and managing an information security risk management program using the MEHARI methodology as a reference framework.

The target population for this examination is (this is a non-exhaustive list):

- Individuals seeking to gain a thorough understanding of MEHARI risk analysis method and MEHARI risk model
- Managers seeking to develop the necessary skills to support organizations in information security risk analysis
- Auditors seeking to gain a thorough understanding of the MEHARI method
- Members of an information security team seeking to advance their skills and gain a thorough understanding on how to evaluate the quality of security services

The exam content covers the following domains:

- **Domain 1:** Fundamental concepts, principles, and approaches of information security risk management based on the MEHARI method
- **Domain 2:** Implementation of an information security risk management program based on the MEHARI method
- **Domain 3:** Information security risk assessment based on the MEHARI method

The content of the exam is divided as follows:

Domain 1: Fundamental concepts, principles, and approaches of information security risk management based on the MEHARI method

Main objective: To ensure that the candidate can understand, interpret and illustrate the main risk management guidelines and concepts related to a risk management framework based on the MEHARI method

Competencies	Knowledge statements
1. Understand and explain the operations of the organization and the development of risk management standards 2. Ability to identify, analyze and evaluate the guidance coming from risk management frameworks for an organization 3. Ability to explain and illustrate the main concepts in risk management 4. Ability to distinguish and explain the difference between information asset, data and record 5. Understand, interpret and illustrate the relationship between the concepts of asset, vulnerability, threat, impact and controls 6. Ability to distinguish the relationship between MEHARI, ISO/IEC 27005, and other related standards	1. Knowledge of the application of the principles of risk management 2. Knowledge of the main standards in risk management 3. Knowledge of the different sources of risk management frameworks for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies 4. Knowledge of the main risk management concepts and terminology 5. Knowledge of the concept of risk and its application in information security 6. Knowledge of the relationship between the concepts of asset, vulnerability, threat, impact and controls 7. Knowledge of the relationship and differences between ISO/IEC 27005 and MEHARI 8. Knowledge of the relationship between the concepts of asset, threat, likelihood, impact and controls

Domain 2: Implementation of an information security risk management program based on the MEHARI method

Main objective: To ensure that the candidate can implement the processes of a risk management reference frameworks based on MEHARI

Competencies	Knowledge statements
1. Ability to understand, analyze needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation and management of a risk management framework 2. Ability to define the document and record management processes needed to support the implementation and the operations of a risk management framework 3. Ability to define and design controls & processes and document them 4. Ability to define and write policies and procedures 5. Ability to implement the required processes of a risk management framework 6. Ability to define and implement appropriate risk management training, awareness and communication plans 7. Ability to define and implement an incident management process based on best practices 8. Ability to transfer a project to operations and manage the change management process	1. Knowledge of the roles and responsibilities of the key actors during the implementation of a risk management framework and in its operation after the end of the implementation project 2. Knowledge of the main organizational structures applicable for the management of the risk within an organization 3. Knowledge of the best practices on document and record management processes and the document management life cycle 4. Knowledge of model-building controls, processes and techniques 5. Knowledge of controls and processes deployment techniques 6. Knowledge of techniques and best practices to write policies, procedures and others types of documents 7. Knowledge of the characteristics and the best practices to conduct risk management training, awareness and communication plans 8. Knowledge of the characteristics and main processes of an information security incident management process based on best practices 9. Knowledge of change management techniques 10. Knowledge of the objectives of a risk management program and risk assessment process

Domain 3: Information security risk assessment based on the MEHARI method

Main objective: To ensure that the candidate can perform a risk assessment in the context of an organization using the MEHARI methodology

Competencies	Knowledge statements
1. Ability to understand and interpret Information Security Risk Management processes according to MEHARI 2. Ability to know and describe several recognized risk assessment methodologies Ability to identify, review and select a Risk Assessment Approach appropriate for a specific organization 3. Ability to plan activities for Risk Assessment and integrate risk assessment to risk management 4. Ability to lead assessment projects and manage multidisciplinary teams 5. Ability to perform risk assessments in various settings and establishments 6. Ability to identify primary and supporting assets of an organization 7. Ability to identify the consequences in terms of confidentiality, integrity and availability of assets 8. Ability to assess the likelihood and determine the level of risk for each identified incident scenario 9. Ability to choose a risk analysis methodology that suits the needs of the organization 10. Ability to calculate the level of risk in terms of the combination of consequences and their likelihood	1. Knowledge of the guidelines and processes from risk management guidelines and frameworks based on MEHARI 2. General knowledge of the main risk assessment methodologies. 3. Knowledge on planning risk assessment projects and activities by ensuring the participation and support of stakeholders throughout the risk assessment process 4. Knowledge on risk assessment projects of a more global and more complex nature 5. Knowledge of information gathering techniques Knowledge on identification of assets, risk sources, vulnerabilities, existing measures, impacts, incident likelihood and the relation between these concepts 6. Knowledge on likelihood assessment and risk level determination for different identified incident scenarios 7. Knowledge of risk level estimation according to the evaluation criteria and the risk acceptance criteria 8. Knowledge on the outcomes of risk analysis and risk prioritization

Based on these 3 domains and their relevance, six (6) questions are included in the exam, as summarized in the following table:

			Leve l of Understanding (Cognitive/Taxonomy) Required					
		Points per Question	Questions that measure Comprehension, Application and Analysis	Questions that measure Synthesis and Evaluation	Number of Questions per competency domain	% of test devoted to each competency domain	Number of Points per competency domain	% of Points per competency domain
Competency/Domains	Fundamental concepts, principles, and approaches of information security risk management based on the MEHARI method	5	X		1	16.67	5	6.67
	Implementation of an information security risk management program based on the MEHARI method	5	X		4	66.67	30	40
		5	X					
		10		X				
		10		X				
	Information security risk assessment based on the MEHARI method	40		X	1	16.67	40	53.33
Total points		75						
Number of Questions per level of understanding			3	3				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			50.00	50.00				

The passing score is established at **70%.**

After successfully passing the exam, candidates will be able to apply for the credentials of PECB Certified MEHARI, depending on their level of experience.

TAKE THE CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the invigilator.

The exam duration is two (2) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be "open book" and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are "open book"; candidates are authorized to use the following reference materials:

- A copy of the MEHARI standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course and
- A hard copy dictionary.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of allowed time-frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, he/she must wait 15 days for the next attempt (1st retake). Retake fee applies.

Note: Students, who have completed the full training but failed the written exam, are eligible to retake the exam once for free within a 12 month period from the initial date of the exam.

- If a candidate does not pass the exam on the second attempt, he/she must wait 3 months (from the initial date of the exam) for the next attempt (2nd retake). Retake fee applies.
- If a candidate does not pass the exam on the third attempt, he/she must wait 6 months (from the initial date of the exam) for the next attempt (3rd retake). Retake fee applies.

After the fourth attempt, a waiting period of 12 months from the last session date is required, in order for candidate to sit again for the same exam. Regular fee applies.

For the candidates that fail the exam in the 2nd retake, PECB recommends to attend an official training in order to be better prepared for the exam.

To arrange exam retakes (date, time, place, costs), the candidate needs to contact the PECB partner who has initially organized the session.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. Identification of assets

Explain why these are the assets with the highest value to the organization. Please also identify whether the following are primary or supporting assets:

Possible answers:

Asset 1: website (primary asset)

Justification of the value: The website of the company is the main marketing tool and supports the selling process.

Asset 2: The two owners (supporting asset)

Justification of the value: They are the ones creating original and innovative products.

2. Identification of risk associated with information security

Identify threats, vulnerabilities and impacts associated with the incident scenarios below and indicate if it is possible that the impacts affect the availability, integrity and/or the confidentiality of the information. Complete the risk matrix.

Possible answers:

Statements	Vulnerabilities	Threats	C	I	A	Potential Impacts
1. The webmaster who designed the corporate Website takes care of the updates and the uploading of the site	Absence of segregation of duties. Only one person is available for this function	Treatment errors Malicious act Webmaster leaves the company or becomes sick		X	X	Website containing erroneous information: loss of credibility Unavailable website: loss in revenues